Przez nieostrożne korzystanie z telefonu można zostać bez grosza

Kategoria: Styl życia
Opublikowano: wtorek, 24, październik 2017 10:44
Artur Duda
Odsłony: 1470

Smartfony w coraz większym stopniu zastępują nasze portfele. Dlatego trzeba je dobrze chronić, gdyż są przepustką do naszych pieniędzy. Za ich pomocą można bowiem ukraść nawet większą kwotę niż ta, jaką zwykle nosimy w portfelu. Telefon może posłużyć przestępcom do kradzieży wszystkich naszych oszczędności. mBank ostrzegał niedawno przed wirusem, który atakuje nasze smartfony i wyłudza informacje potrzebne do kradzieży pieniędzy z konta. Expander podpowiada, jak bezpiecznie korzystać z płatności mobilnych.

Kiedyś płacenie telefonem polegało na zadzwonieniu na infolinię banku i zlecenie tam przelewu. Dziś aż 57% Polaków ma smartfona, czyli telefon, na którym można zainstalować różnego rodzaju programy np. aplikacje bankowe. Do tych najnowocześniejszych zalogujemy się już odciskiem palca. Pozwalają one nie tylko na robienie przelewów. Telefon może np. działać dokładnie tak jak karta zbliżeniowa. Jeśli włączymy odpowiednie funkcje, do terminalu w sklepie możemy zbliżyć telefon zamiast karty. Wg CBOS z takiej możliwości korzysta już 5% Polaków. Na smartfonie możemy również włączyć usługę BLIK, która wyświetla kody pozwalające m. in. wypłacać pieniądze z bankomatów. Ma ona już 3,8 mln użytkowników. Jest też kilka różnych sposobów płacenia telefonem za zakupy w sklepach internetowych.

Smartfony są tak naprawdę małymi komputerami, co oznacza, że mogą je atakować wirusy. Niedawno ostrzegał przed tym mBank. Wirus rozpoznawał, kiedy ktoś włączał aplikację tego banku i wyświetlał komunikaty w taki sposób, że wydawało się, że pochodzą one od banku. Prosił o podanie nr telefonu, PINu do logowania się do aplikacji czy loginu i hasła do logowania się w bankowości internetowej. Ktoś, kto podałby te informacje, dałby przestępcom możliwość swobodnego dokonywania wypłat z jego konta.

Antywirus to nie wszystko

Podobnie jak na komputerze, tak i na telefonie warto zainstalować program antywirusowy. Trzeba jednak dodać, że i on nie da 100% bezpieczeństwa. Dlatego najlepiej jednocześnie stosować kilka zasad bezpieczeństwa. Przede wszystkim nie należy instalować na telefonie programów pobranych z innych źródeł niż oficjalne sklepy z aplikacjami (Google Play, App Store). Takie sklepy sprawdzają bowiem, czy udostępniane przez nie programy są bezpieczne. Domyślnie zwykle telefon ma włączoną blokadę chroniącą przed nieautoryzowanymi aplikacjami. Jeśli więc nagle pojawi nam się komunikat z pytaniem, czy na pewno chcemy zainstalować aplikację z niezaufanego źródła, powinna nam się zapalić czerwona lampka.

Warto też unikać otwierania załączników do maili czy klikania w linki zawarte w korespondencji elektronicznej, jeśli taką wiadomości otrzymaliśmy od nieznanych nam osób. Niestety przestępcy czasami podszywają się pod różnego rodzaju firmy czy instytucje. Bywa więc, że trudno zorientować się, że to pułapka. Dlatego tak ważny jest program antywirusowy i pozostawienie włączonej blokady instalacji aplikacji z nieznanych źródeł.

Warto ustawić również odblokowanie ekranu naszego urządzenia za pomocą hasła, PINu czy odcisku palca. Jest to szczególnie istotne, jeśli na telefonie mamy włączoną funkcję płatności zbliżeniowych. Jednak nawet jeśli nie korzystamy z tego sposobu płatności, to lepiej stosować taką blokadę.
W telefonie zwykle mamy bowiem mnóstwo informacji (zdjęć, kontaktów, aplikacji), których nie chcielibyśmy zapewne przekazywać niepowołanym osobom. Wszystkie PINy czy hasła, niezależnie czy służą do odblokowania ekranu czy do logowania się do aplikacji bankowych nie powinny też być zbyt proste - np. 1111 czy 1234 mogą zostać dość łatwo złamane. Najlepiej też, aby były one inne do różnych aplikacji. Jeśli bowiem w jakiś sposób przestępcom uda się np. podejrzeć jaki PIN odblokowuje ekran

Phoca PDF

naszego telefonu, to ten kod zapewne spróbują również wykorzystać żeby zalogować się do naszej bankowej aplikacji mobilnej.

Źródło: Newsrm.tv, wypowiedź: Jarosław Sadowski, główny analityk firmy Expander.

Phoca PDF